

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-133384

(43)Date of publication of application : 10.05.2002

(51)Int.Cl.

G06K 19/073

B42D 15/10

G06F 1/00

G06F 15/00

G06F 17/60

(21)Application number : 2000-318428

(71)Applicant : NTT DATA CORP

(22)Date of filing : 18.10.2000

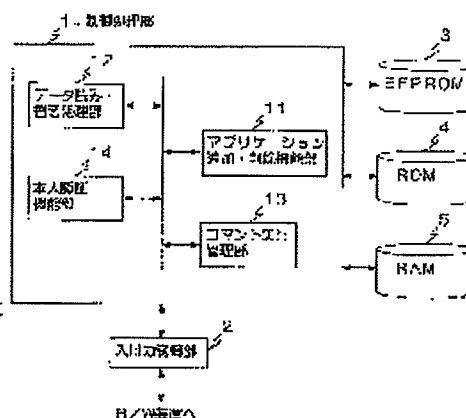
(72)Inventor : IINO TORU  
IWASE FUMIYUKI

## (54) IC CARD, REGISTER DEVICE AND SERVICE PROVIDING SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an IC card, a register device and a service providing system that ensure sharing of a principal authentication function in the IC card among a plurality of services and permit a service user's own selection of a plurality of principal authentication methods to a degree keeping safety intact.

SOLUTION: A principal authentication function part 14 uses an authentication method recorded in an EEPROM 3 to compare an authentication template for principal specification recorded in the EEPROM 3 and information externally input when a command execution management part 13 executes processing of an application program, and then executes an authentication of the IC card user in an authentication method specified by the application program. Application programs run on the IC card are managed by an application addition and deletion function part 11, and a register of authentication information including an authentication method requested by an application program and an authentication template is managed by a data reading and writing part 12.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-133384

(P2002-133384A)

(43) 公開日 平成14年5月10日 (2002.5.10)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード <sup>*</sup> (参考)
G 0 6 K 19/073		B 4 2 D 15/10	5 2 1 2 C 0 0 5
B 4 2 D 15/10	5 2 1	G 0 6 F 15/00	3 3 0 G 5 B 0 3 5
G 0 6 F 1/00		17/60	2 2 2 5 B 0 5 5
15/00	3 3 0	G 0 6 K 19/00	P 5 B 0 7 6
17/60	2 2 2	G 0 6 F 9/06	6 6 0 E 5 B 0 8 5
審査請求 未請求 請求項の数10 O L (全 26 頁)			

(21) 出願番号 特願2000-318428(P2000-318428)

(22) 出願日 平成12年10月18日 (2000.10.18)

(71) 出願人 000102728

株式会社エヌ・ティ・ティ・データ

東京都江東区豊洲三丁目3番3号

(72) 発明者 飯野 徹

東京都江東区豊洲三丁目3番3号 株式会

社エヌ・ティ・ティ・データ内

(72) 発明者 岩瀬 史幸

東京都江東区豊洲三丁目3番3号 株式会

社エヌ・ティ・ティ・データ内

(74) 代理人 100064908

弁理士 志賀 正武 (外2名)

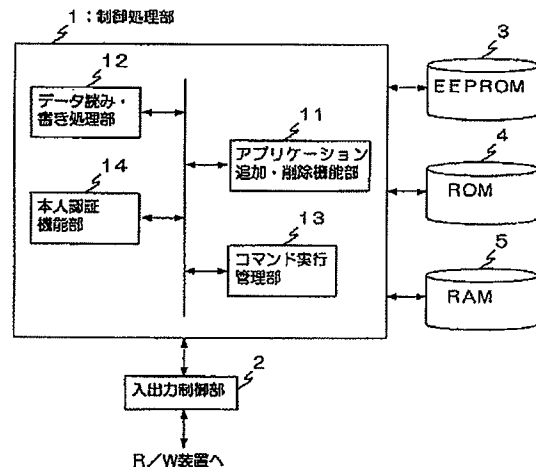
最終頁に続く

(54) 【発明の名称】 ICカード、登録装置、及びサービス提供システム

(57) 【要約】

【課題】 複数のサービスから、ICカード内の本人認証機能を共有し、サービス利用者自身が複数の本人認証方法を、安全性を損なわない範囲で選択できるICカード、登録装置、及びサービス提供システムを提供する。

【解決手段】 本人認証機能部14は、EEPROM3に記録された認証方法を用いて、EEPROM3に記録された本人を特定する認証用テンプレートと、コマンド実行管理部13がアプリケーションプログラムの処理を実行する際に外部より入力された情報とを比較して、アプリケーションプログラムが指定する認証方法によるICカード使用者の認証を行う。ICカード上で実行されるアプリケーションプログラムは、アプリケーション追加・削除機能部11により管理され、アプリケーションプログラムが要求する認証方法や認証用テンプレート等を含む認証情報の登録はデータ読み・書き処理部12により管理される。



## 【特許請求の範囲】

【請求項1】 ICカード上に記録されたアプリケーションプログラムによりサービスを提供するICカードであって、

前記ICカードで実行される複数の前記アプリケーションプログラム、及び前記アプリケーションプログラムを実行するための認証方法と認証データを含む認証情報を記録する記録手段と、

前記記録手段に記録された認証方法を用いて、前記記録手段に記録された本人を特定する認証用データと、前記記録手段に記録されたいずれかのアプリケーションプログラムの処理を実行する際に外部より入力された情報とを比較することによりICカード使用者の認証を行う本人認証手段と、

前記本人認証手段において認証が行われることにより前記記録手段に記録された実行対象となるアプリケーションプログラムの処理を実行するコマンド実行手段と、を設けたことを特徴とするICカード。

【請求項2】 前記本人認証手段は、前記認証方法の実行結果を予め設定された点数により取得する手段と、

予め設定された優先順位に従い実行される複数の前記認証方法の実行結果として出力された前記点数を加算する手段と、

加算された前記点数とアプリケーションプログラムの指定する所定の点数とを比較する手段と、を更に含み、

前記アプリケーションプログラムの指定する所定の点数を満たした時点で、前記アプリケーションに認証の正常終了を通知することを特徴とする請求項1に記載のICカード。

【請求項3】 前記本人認証手段は、前記認証方法の実行結果を予め設定された点数により取得する手段と、

前記認証方法の実行結果として出力された現在の点数と次に実行するアプリケーションプログラムの指定する所定の点数とを比較する手段と、

比較の結果、前記アプリケーションプログラムの指定する所定の点数が前記現在の点数より大きい場合、前記アプリケーションプログラムに指定された認証方法を実行し、該認証方法による点数を新しい現在の点数として記録・更新する手段と、

を更に含み、

認証結果による現在の点数が、前記アプリケーションプログラムの指定する所定の点数を満たしていた場合、該アプリケーションプログラムの指定する認証方法の実行を省略することを特徴とする請求項1に記載のICカード。

【請求項4】 前記本人認証手段は、認証に使用する前記認証用データが複数記録されている

場合、予め設定された優先順位により前記認証方法に用いる認証用データを選択することを特徴とする請求項1から請求項3のいずれかに記載のICカード。

【請求項5】 前記本人認証手段は、認証の失敗により、前記認証データが使用停止となっても、他の認証データを用いた本人認証により本人を確認できる場合、使用停止となった該認証データを復元する手段を更に含むことを特徴とする請求項1から請求項4のいずれかに記載のICカード。

【請求項6】 請求項1から請求項5のいずれかに記載のICカードに、認証データを含む認証情報を登録する認証情報登録装置であって、

ICカードが認証情報登録装置を正当な接続先であると確認するための登録認証を実行する登録認証手段と、前記登録認証が正常な場合、登録可能な認証方法を表示し、利用者に希望する前記認証方法を選択させる選択手段と、

選択された前記認証方法と前記認証情報を前記ICカードへ登録する登録手段と、

を設けたことを特徴とする認証情報登録装置。

【請求項7】 請求項1から請求項5のいずれかに記載のICカードに、ICカードで実行するアプリケーションプログラムを登録するアプリケーションプログラム登録装置であって、

アプリケーション用鍵によりアプリケーションプログラムの認証を実行する認証手段と、

前記アプリケーション鍵による認証が正常な場合、ICカードに登録された認証方法により本人認証を行わせる確認手段と、

ICカードが実行した本人認証が正常な場合、追加可能なアプリケーションプログラムを表示して、利用者に希望するアプリケーションプログラムを選択させる選択手段と、

選択されたアプリケーションプログラムを登録・削除する登録・削除手段と、

を設けたことを特徴とするアプリケーションプログラム登録装置。

【請求項8】 請求項1から請求項5のいずれかに記載のICカードを用いたサービス提供システムであって、

ICカードの発行と利用者の管理を行う顧客管理サーバと、

利用者がICカードを利用するための、自宅、あるいは店舗に用意されたクライアント端末と、

を設けたことを特徴とするサービス提供システム。

【請求項9】 利用者が街頭でICカードを入手するためのICカード自動販売機と、

ICカード自動販売機の販売履歴と利用者を管理するICカード販売管理サーバと、

を更に設けたことを特徴とする請求項8に記載のサービス提供システム。

【請求項10】 ICカード上に記録されたアプリケーションプログラムによりサービスを提供するICカードにおけるICカード使用者の認証方法であって、前記ICカードで実行される複数の前記アプリケーションプログラム、及び前記アプリケーションプログラムを実行するための認証方法と認証データを含む認証情報を記録するICカード上の記録手段に記録された認証方法を用いて、前記記録手段に記録された本人を特定する認証用データと、前記記録手段に記録されたいずれかのアプリケーションプログラムの処理を実行する際に外部より入力された情報とを比較することによりICカード使用者の認証を行う本人認証処理と、前記本人認証処理において認証が行われることにより前記記録手段に記録された実行対象となるアプリケーションプログラムの処理を実行するコマンド実行処理と、を含むことを特徴とするICカード使用者の認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、人間の生体情報による認証を含む、複数の認証方法を利用するICカード、登録装置、及びサービス提供システムに関する。

【0002】

【従来の技術】従来、本人の生体的特徴を利用して、本人を電子的に認証する技術の一つにバイオメトリクス技術がある。認証方法は、主に以下のように行う。

(1) あらかじめ本人の生体的特徴(経年変化が少なく、個人毎に特有の特徴があるもの)をデジタル化し登録する。

(2) 照合時に認証する人の生体的特徴をスキャナなどで取り込みデジタル化し、あらかじめ登録したデータとの類似度を計算し、類似度が一定以上の場合、本人とする。

このようなバイオメトリクス技術をシステムに導入する際には、個人の生体情報を安全に管理する仕組みが必要である。なぜなら個人の生体情報は、プライバシー性の高い情報であり、変更ができないという特性を持っているからである。この問題を補完する一つの方法にICカードなどの個人の携帯型機器と組み合わせる方法がある。すなわち、個人毎のICカードに生体情報を格納し、管理させることで、プライバシーを守ることを可能とする。またICカードに生体情報を格納し、小型の照合装置を組み合わせることで、認証サーバを利用せずにローカルで比較的安全な認証を可能とする技術も提案されている。これらの技術は、比較的人数の場合であれば、小型の照合装置に複数人の生体情報を管理させる方法でシステム構築可能である。しかし、多人数で複数の照合装置を利用する場合、生体情報を一括管理することは難しい。そのため、個人毎のICカードに生体情報を格納し、管理させる方法が提案されている。

【0003】

【発明が解決しようとする課題】このような個人が所有する携帯機器の利用や、機器を用いて行う認証行為に対して、本人であるかを認証する方法には、パスワードを生体情報と組み合わせて利用するものがある。しかし、パスワードは、忘失による問題や盗難によるなりすましの危険性があるという問題があった。また、生体情報を利用する場合、怪我等の使用部位の状態、体調、更には指紋認証を例にとると、生まれつき指紋が薄くて認証には適さない等、生まれながらの特性により完全な本人認証ができない場合があるという問題があった。更に、これらの欠点を補完するためには複数の認証方法を組み合わせる必要がある。しかし、一般的に本人認証方法は、サービス提供者毎に固定的に決められている。そのため、本人認証をサービス毎に繰り返す必要があり、無駄が多いという問題があった。

【0004】本発明は、上記問題点を鑑みてなされたもので、サービス提供者毎に別々の本人認証方法を用いるのではなく、複数のサービスから、ICカード内の本人認証機能を共有することで、本人認証機能の無駄を省くことを可能とし、かつ、サービス利用者自身が複数の本人認証方法を、安全性を損なわない範囲で選択できる仕組みにより、本人認証に必要な情報の登録及び変更を容易に実現することを可能とするICカード、登録装置、及びサービス提供システムを提供することを目的とする。

【0005】

【課題を解決するための手段】上記問題点を解決するために、本発明は、ICカード上に記録されたアプリケーションプログラムによりサービスを提供するICカードであって、ICカードで実行される複数のアプリケーションプログラム、及びアプリケーションプログラムを実行するための認証方法と認証データを含む認証情報を記録する記録手段と、記録手段に記録された認証方法を用いて、記録手段に記録された本人を特定する認証用データと、記録手段に記録されたいずれかのアプリケーションプログラムの処理を実行する際に外部より入力された情報とを比較することによりICカード使用者の認証を行う本人認証手段と、本人認証手段において認証が行われることにより記録手段に記録された実行対象となるアプリケーションプログラムの処理を実行するコマンド実行手段とを設けたことを特徴とする。以上の構成により、ICカードで実行するアプリケーションプログラム、及びアプリケーションプログラムが要求する本人認証に必要な情報の登録及び変更を容易に実現することを可能とする。

【0006】本発明は、上記ICカードにおいて、本人認証手段は、認証方法の実行結果を予め設定された点数により取得する手段(例えば実施の形態のステップS102)と、予め設定された優先順位に従い実行される複

数の認証方法の実行結果として出力された点数を加算する手段（例えば実施の形態のステップS106）と、加算された点数とアプリケーションプログラムの指定する所定の点数とを比較する手段（例えば実施の形態のステップS103またはステップS107）とを更に含み、アプリケーションプログラムの指定する所定の点数を満たした時点で、アプリケーションに認証の正常終了を通知することを特徴とする。以上の構成により、ICカードで実行されるアプリケーションプログラムの内容に関わらず、複数の認証方法を利用者が指定する優先順位により選択して実行することを可能とする。

【0007】本発明は、上記ICカードにおいて、本人認証手段は、認証方法の実行結果を予め設定された点数により取得する手段（例えば実施の形態のステップS123）と、認証方法の実行結果として出力された現在の点数と次に実行するアプリケーションプログラムの指定する所定の点数とを比較する手段（例えば実施の形態のステップS128からステップS130）と、比較の結果、アプリケーションプログラムの指定する所定の点数が現在の点数より大きい場合、アプリケーションプログラムに指定された認証方法を実行し、該認証方法による点数を新しい現在の点数として記録・更新する手段（例えば実施の形態のステップS131）とを更に含み、認証結果による現在の点数が、アプリケーションプログラムの指定する所定の点数を満たしていた場合、該アプリケーションプログラムの指定する認証方法の実行を省略することを特徴とする。以上の構成により、ICカードで実行される複数のアプリケーションプログラムが認証方法の結果を共有することを可能とする。

【0008】本発明は、上記ICカードにおいて、本人認証手段は、認証に使用する認証用データが複数記録されている場合、予め設定された優先順位により認証方法に用いる認証用データを選択することを特徴とする。以上の構成により、怪我をして指紋認証ができない場合等に、認証方法の実行順序を変更することを可能とする。

【0009】本発明は、上記ICカードにおいて、本人認証手段は、認証の失敗により、認証データが使用停止となっても、他の認証データを用いた本人認証により本人を確認できる場合、使用停止となった該認証データを復元する手段（例えば実施の形態のステップS141からステップS153）を更に含むことを特徴とする。以上の構成により、利用者や管理者が安全かつ容易にICカードの管理を行い、ICカードを継続利用することを可能とする。

【0010】本発明は、上記ICカードに、認証データを含む認証情報を登録する認証情報登録装置であって、ICカードが認証情報登録装置を正当な接続先であると確認するための登録認証を実行する登録認証手段（例えば実施の形態のステップS2）と、登録認証が正常な場合、登録可能な認証方法を表示し、利用者に希望する認

証方法を選択させる選択手段（例えば実施の形態のステップS5からステップS6）と、選択された認証方法と認証情報をICカードへ登録する登録手段（例えば実施の形態のステップS7）とを設けたことを特徴とする。以上の構成により、利用者がICカードに希望する認証方法を安全かつ容易に登録することを可能とする。

【0011】本発明は、上記ICカードに、ICカードで実行するアプリケーションプログラムを登録するアプリケーションプログラム登録装置であって、アプリケーション用鍵によりアプリケーションプログラムの認証を実行する認証手段（例えば実施の形態のステップS43）と、アプリケーション鍵による認証が正常な場合、ICカードに登録された認証方法により本人認証を行わせる確認手段（例えば実施の形態のステップS45）と、ICカードが実行した本人認証が正常な場合、追加可能なアプリケーションプログラムを表示して、利用者に希望するアプリケーションプログラムを選択させる選択手段（例えば実施の形態のステップS48からステップS49）と、選択されたアプリケーションプログラムを登録・削除する登録・削除手段（例えば実施の形態のステップS50）とを設けたことを特徴とする。以上の構成により、利用者がICカードに希望するアプリケーションプログラムを安全かつ容易に登録することを可能とする。

【0012】本発明は、上記ICカードを用いたサービス提供システムであって、ICカードの発行と利用者の管理を行う顧客管理サーバ（例えば実施の形態の顧客管理サーバ101）と、利用者がICカードを利用するための、自宅、あるいは店舗に用意されたクライアント端末（例えば実施の形態のクライアント端末103）とを設けたことを特徴とする。以上の構成により、利用者がクライアント端末からの操作でICカードの発行やICカードの利用を行うことを可能とする。

【0013】本発明は、上記サービス提供システムにおいて、利用者が街頭でICカードを入手するためのICカード自動販売機（例えば実施の形態のICカード自動販売機105）と、ICカード自動販売機の販売履歴と利用者を管理するICカード販売管理サーバ（例えば実施の形態のICカード販売管理サーバ106）とを更に設けたことを特徴とする。以上の構成により、利用者が街頭の端末からICカードを入手することを可能とする。

【0014】本発明は、ICカード上に記録されたアプリケーションプログラムによりサービスを提供するICカードにおけるICカード使用者の認証方法であって、ICカードで実行される複数のアプリケーションプログラム、及びアプリケーションプログラムを実行するための認証方法と認証データを含む認証情報を記録するICカード上の記録手段に記録された認証方法を用いて、記録手段に記録された本人を特定する認証用データと、記

10

20

30

40

50

録手段に記録されたいずれかのアプリケーションプログラムの処理を実行する際に外部より入力された情報とを比較することによりICカード使用者の認証を行う本人認証処理と、本人認証処理において認証が行われることにより記録手段に記録された実行対象となるアプリケーションプログラムの処理を実行するコマンド実行処理とを含むことを特徴とする。

【0015】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態について説明する。図1は、本実施の形態のICカード上に構成される機能ブロックを説明するブロック図である。図1において、符号1は、本実施の形態のICカードの動作を制御する制御処理部を示す。符号2は、制御処理部1とICカードの情報を読み書きするICカードのR/W(Read/Write)装置を接続する入出力制御部を示す。符号3は、ICカード上で実行するアプリケーションプログラムや認証方法、及び認証用テンプレート(パスワードや認証用生体データ等のデータ)等を含む認証情報を記録するためのEEPROM(Electrically Erasable and Programmable ROM:電氣的書き換え可能な不揮発性メモリ)を示す。符号4は、制御処理部1で実行される本実施の形態のICカードの制御プログラムを予め記録してあるROM(Read Only Memory)を示す。符号5は、制御処理部1で扱われる一時的なデータを記録するためのRAM(Random Access Memory)を示す。なお、本実施の形態のICカードとICカードのR/W装置とのインターフェースは接触型のみでなく、無線等を用いた非接触型により実現することも可能であり、この場合、入出力制御部2は無線系の回路を含むものとする。また、EEPROM3は、フラッシュメモリ(Flash Memory:電氣的書き換え可能な半導体不揮発性メモリ)を用いても良い。

【0016】また、制御処理部1は、アプリケーション追加・削除機能部11と、データ読み・書き処理部12と、コマンド実行管理部13と、本人認証機能部14とから構成されている。アプリケーション追加・削除機能部11は、EEPROM3に記録されるアプリケーションプログラムの追加、及び削除を管理する。データ読み・書き処理部12は、EEPROM3に記録される認証方法や認証用テンプレート(パスワードや認証用生体データ等のデータ)等を含む認証情報の登録、及びメンテナンスを行う。コマンド実行管理部13は、アプリケーション追加・削除機能部11によりICカード上に記録されたアプリケーションプログラムの処理を実行する。本人認証機能部14は、EEPROM3に記録された認証方法を用いて、EEPROM3に記録された本人を特定する認証用テンプレート(パスワードや認証用生体データ等のデータ)と、コマンド実行管理部13がアプリケーションプログラムの処理を実行する際に外部より入力された情報とを比較することによりICカード使用者

の認証を行う。

【0017】次に、図2、及び図3を用いてEEPROM3に記録される情報の構成を説明する。図2、及び図3は、本発明の実施の形態のICカード上のEEPROM3に記録される情報の構成を説明する模式図である。図2、及び図3において、EEPROM3に記録される情報の種類は大別すると次のように分類される。

(1)アプリケーションプログラム

(2)認証方法に関する情報

(3)鍵データ

(4)その他情報

それぞれについて更に詳細に説明すると、(1)アプリケーションプログラムとしては、“アプリケーションプログラム1～N”と、アプリケーションプログラムそれぞれについて、アプリケーションプログラムが本人認証機能部14による認証機能を使用するか否かを示した“a. 本人認証機能使用フラグ”と、アプリケーションプログラムが必要な本人認証のレベルを意味する“b. 本人確認レベル”が記録可能である。なお、“本人確認レベル”についての詳細は後述する。また、(2)認証方法に関する情報としては、認証方法1～Nのそれぞれについて、M個の“本人認証用テンプレート(パスワードや認証用生体データ等のデータ)”と、認証方法のパラメータとして、“しきい値、テンプレート優先順位、各テンプレートのロック・アンロック再試行回数、アンロック回数上限値、ロック回数上限値、組み合わせパラメータ”等が記録可能である。ここで、“しきい値”は、本人認証の際に入力されたテンプレートと、あらかじめカード内に設定したテンプレートとの類似度を算出し、その値がある値以上か否かにより、本人か否かを判断する時に利用する基準値である。“テンプレート優先順位”は、各々の本人認証方法で利用するテンプレートを、複数ICカード内に格納する場合に、どのテンプレートを優先的に使用するかというパラメータである。なお、当該テンプレートは、1人のものを複数入れるだけでなく、複数人のテンプレートを入れてもよい。“組み合わせパラメータ”は、一度に複数のテンプレートを本人認証の際に使用する場合、その組み合わせ方法を示すパラメータである。

【0018】更に、入力されたテンプレートと登録されているテンプレートを比較し、認証が失敗した回数をカード内に記録する。“ロック回数上限値”を越えて認証が失敗すると、当該テンプレートをロックし、当該テンプレートを使用できない状態にする。また“ロック再試行回数”は、“ロック回数上限値”から認証が失敗した数を引いた残り回数を示し、ロックまでの再試行可能回数を表す。なお、ロックをしない設定にするには、“ロック回数上限値”をゼロにすることにより可能とする。また、生体状態の変化により、仮に一つのテンプレートが「ロック回数上限値」を越えて、ロックした場合で

も、他のテンプレートで本人認証がOKになった場合、当該テンプレートをアンロックし、再度使用可能にすることができることとする。”アンロック回数上限値”は、アンロックが可能な上限回数を示し、一度アンロックをすると、”アンロック再試行回数”を1ずつ減少し、0になった段階でアンロックを実行不可能とする。また(3)鍵データとしては、アプリケーションプログラムを追加する際に使用する”アプリケーション追加鍵データ”と、アプリケーションプログラムを削除する際に使用する”アプリケーション削除鍵データ”と、ICカード発行者がICカード内のメンテナンスを行う際に使用する”発行者用鍵データ”と、ICカード管理者がICカード内のメンテナンスを行う際に使用する”メンテナンス用鍵データ”等が記録可能である。また、(4)その他情報としては、アプリケーションプログラムが実行した本人認証の結果である”カード側本人確認レベル”と、ICカード内に設定している複数の認証方法の一覧を示す”カード側認証方法リスト”と、複数の認証方法が設定されている場合に、複数の認証方法を行う順番を示した”認証方法優先順位”とICカードの有効期限を示す”カード有効期限”等が記録可能である。なお、カード側本人確認レベル”は本人認証が成功した段階でセットされ、ICカードをリセットした段階でクリアされる。

【0019】次に、図面を用いて、本実施の形態の動作を説明する。まず、図4のフローチャートを用いて、専用の登録端末によるICカードへの本人認証機能の登録動作を説明する。図4において、まずユーザのICカード入手意志を確認する(ステップS1)。ステップS1において、ユーザにICカード入手の意志がある場合(ステップS1のYES)、ICカードに個人の認証データ(パスワードや生体情報など)を登録するためのICカードの登録認証を実行する(ステップS2)。登録認証は、ICカードが登録端末を正当な接続先であると確認するために行い、カードへの書き込みは、認証が成功した段階で可能となる。なお、認証動作の詳細は後述する。次に、ICカードの登録認証が正常に終了したか否かを判定する(ステップS3)。ステップS3において、ICカードの登録認証が正常に終了していた場合(ステップS3のYES)、認証方法の登録を開始する(ステップS4)。そして、ユーザ自身が複数の認証方法の中から、適当な認証方法を選択できるように、登録可能な認証方法を表示する(ステップS5)。例えば、複数のスキャナやカメラなどがついている登録端末の場合、複数の認証方法をユーザ自身が選択することができる。次に、ユーザに希望の認証方法があるか否かを判断させる(ステップS6)。ステップS6において、ユーザが希望の認証方法があると判断した場合(ステップS6のYES)、認証情報を登録する(ステップS7)。認証情報は、スキャナやカメラなどを用いて得た情報か

ら特徴情報を抽出し、特徴情報の品質が良いと判断した段階で成功とし、当該データをICカードへ書き込む。そして、認証情報の登録が成功したか否かを判定し(ステップS8)、登録が成功していた場合(ステップS8のYES)、カード内の認証方法リストを書き換え、ICカードを排出して(ステップS9)、ICカードへの本人認証機能の登録動作を終了する。

【0020】一方、ステップS3において、ICカードの登録認証が正常に終了していなかった場合(ステップS3のNO)、ICカードは偽造されていると判断し、システムを停止してカード発行動作を停止する(ステップS10)。また、ステップS7において、認証情報の登録が成功していなかった場合(ステップS8のNO)、再度登録するか否かをユーザに入力させる(ステップS11)。ステップS11において、再度登録するとユーザが入力した場合(ステップS11のYES)、ステップS5へ戻り、上述の動作を繰り返す。ステップS11において、再度登録しないとユーザが入力した場合(ステップS11のNO)、ICカードへの本人認証機能の登録動作を終了する。上述のように、登録の際には複数回の中から良い状態のものを選択して登録する。登録が失敗する場合は、ステップS5へ戻り、登録可能な認証方法を選択する。ここでは、認証方法の詳細を設定することも可能である。たとえば複数の認証方法を使う場合の順番や方法の組み合わせ方、テンプレートの順番や組み合わせ方である。また、使用したい認証方法の優先順位も設定できる。更に、上述の方法では、カード入手時に認証方法が設定されていないが、入手時点であらかじめ既に認証方法が設定されていても良い。その場合ICカードへの登録認証の前に、設定された認証方法による照合を行い、認証が成功した段階で認証方法の追加・削除・優先順位の変更を可能とする。認証が失敗した場合はカードを排出する。

【0021】次に、図5のシーケンス図を用いて、本人認証機能の登録時のICカードへの登録認証動作の一例を説明する。登録認証動作は、まず登録端末からICカードへ乱数生成要求を送信する(ステップS21)。乱数生成要求を受信したICカードは乱数を生成し(ステップS22)、生成した乱数Aを登録端末へ送信する(ステップS23)。登録端末では乱数Aを秘密鍵で暗号化し(ステップS24)、ICカードへ送信する(ステップS25)。ICカードでは、受信した暗号文を復号化し(ステップS26)、復号化した乱数を生成した乱数Aと比較する(ステップS27)。比較の結果、乱数が一致した場合、登録フラグを立てて(ステップS28)、登録端末へ正常終了を返信する(ステップS29)。また、比較の結果、乱数が一致しない場合、登録端末へエラーを返信する(ステップS30)。

【0022】次に、図6のフローチャートを用いて、専用のアプリケーション登録・削除端末によるICカード

へのアプリケーションプログラムの登録・削除動作を説明する。図6において、まずアプリケーション登録・削除端末にICカードを挿入させる(ステップS41)。次に、挿入されたICカードの有効期限が期限内か否かを判定する(ステップS42)。ステップS42において、ICカードが有効期限内であった場合(ステップS42のYES)、アプリケーション鍵による認証を行う(ステップS43)。なお、アプリケーション鍵による認証の詳細は後述する。そして、認証が成功したか否かを判定し(ステップS44)、認証が成功していれば(ステップS44のYES)、ICカードに、図4に示した本人認証機能の登録により登録した本人認証を実行させる(ステップS45)。次に、本人認証が成功したか否かを判定し(ステップS46)、認証が成功していれば(ステップS46のYES)、ICカード内に登録されている現在のアプリケーションプログラムの登録状況を表示する(ステップS47)。また、追加可能なアプリケーションプログラムの一覧を表示する(ステップS48)。次に、ユーザにアプリケーションプログラムの登録・削除を行うか否かを入力させ(ステップS49)、ユーザがアプリケーションプログラムの登録・削除を行うと入力した場合(ステップS49のYES)、アプリケーションプログラムの登録・削除を行う(ステップS50)。そして、アプリケーションプログラムの登録・削除が成功したか否かを判定し(ステップS51)、成功していれば(ステップS51のYES)、ステップS49へ戻り、更に、ユーザにアプリケーションプログラムの登録・削除を行うか否かを入力させる。

【0023】一方、ステップS42において、ICカードが有効期限内でなかった場合(ステップS42のNO)、ICカード内に登録してあるアプリケーション情報をセンタに送信し(ステップS52)、再度ICカードを入手する際に使用する。また、期限切れのICカードは、カード内の本人確認用データを削除し、ソフトウェア的またはハードウェア的にカードを再度使用できない状態にして廃棄する(ステップS53)。

【0024】また、ステップS44においてアプリケーション鍵による認証が失敗であると判定した場合(ステップS44のNO)、ICカード側またはシステム側の問題であるため、カード内のアプリケーション情報を読み出し、不正カード情報をセンタへ送信する(ステップS54)。そして、カード内の登録や削除の鍵をロックさせ(ステップS55)、ICカードの排出を行う(ステップS56)。更に、ステップS49において、ユーザがアプリケーションプログラムの登録・削除を行わないと入力した場合(ステップS49のNO)、あるいは、ステップS51において、アプリケーションプログラムの登録・削除が失敗したと判定した場合(ステップS51のNO)、ICカードの排出を行う(ステップS56)。なお、アプリケーションプログラムを追加する

時点で、当該アプリケーションプログラム内にセットされている本人確認レベルが、カード側認証方法リストにない場合は、アプリケーションプログラムをダウンロードした直後にICカードより、「ない」という意味のレスポンスをアプリケーション登録・削除端末に出しても良い。

【0025】次に、図7と図8のシーケンス図を用いて、アプリケーションの登録・削除時のアプリケーション鍵による認証動作の一例を説明する。図7において、まず、アプリケーション登録・削除端末からICカードへアプリケーションIDを送信する(ステップS61)。次に、アプリケーションIDのチェックコードにより、ICカード内に記録されているアプリケーションIDとの重複をチェックする(ステップS62)。もし、チェックがOKの場合、ICカード内にフラグを立てて(ステップS63)、アプリケーション登録・削除端末へ正常終了を返信する(ステップS64)。もし、チェックがNGの場合、アプリケーション登録・削除端末へエラーを返信する(ステップS65)。次に、アプリケーション登録・削除端末からICカードへ乱数生成要求を送信する(ステップS66)。乱数生成要求を受信したICカードは、乱数を生成し(ステップS67)、生成した乱数Bをアプリケーション登録・削除端末へ送信する(ステップS68)。

【0026】乱数Bを受信したアプリケーション登録・削除端末は、乱数Bとアプリケーションプログラムのハッシュ値を秘密鍵で暗号化する(ステップS69)。次に、暗号文とアプリケーションプログラム自身(アプリケーションプログラムの登録時のみ、削除時は暗号文のみ)をICカードへ送信する(ステップS70)。暗号文を受信したICカードは、受信した暗号文を復号化し(ステップS71)、復号化した乱数を生成した乱数Bと比較する(ステップS72)。次に、図8において、アプリケーションプログラム登録時は、復号化したハッシュ値と送信されたアプリケーションプログラムのハッシュ値とを比較する(ステップS73)。アプリケーションプログラム削除時は、復号化したハッシュ値とICカード内に記録されたアプリケーションプログラムのハッシュ値とを比較する(ステップS74)。そして、比較の結果、乱数B及びハッシュ値が一致する場合、アプリケーションプログラムの登録、または削除を実行する(ステップS75)。比較の結果、乱数B及びハッシュ値が一致しない場合、アプリケーション登録・削除端末へエラーを返信する(ステップS76)。

【0027】次に、表1を用いて、本実施の形態のICカード上で実行される認証方法毎の本人確認レベルの一例を説明する。“本人確認レベル”は、アプリケーションプログラムが必要とする本人認証のセキュリティレベルを意味する。

【表1】



認証方法	本人確認 レベル
指紋照合 スコア60%以上	13
指紋照合 スコア40%以上	8
指紋照合 スコア30%以上	6
PIN照会 完全一致	10
PIN照会 1桁間違い	1
PIN照会 全桁間違い	-5
生年月日の入力	1
音声認証 スコア30%以上	8
音声認証 スコア20%以上	6
正当なカードかどうか チェックする	3

表1には、認証方法の種類と、それぞれについての本人確認レベルが1対1で記録されている。例を挙げて説明すると、指紋照合による認証方法において、スコアが60%以上で指紋が一致するのは非常に厳しい条件となるので、その本人確認レベルは13ポイントとして高く設定されている。また、生年月日のような情報は簡単に他人に知られてしまうので、生年月日の入力は本人確認レベルが1ポイントとして低く設定されている。このように本人確認レベルは、難易度で分類された認証方法毎に

アプリケーションプログラムが必要とする本人認証のセキュリティレベルをポイントで表し、難易度が高い程、そのポイントも高く設定されている。

【0028】以上を踏まえて、次に、図9のフローチャートを用いて、本実施の形態のICカードで実行されるアプリケーションが1つの認証方法を実行する場合の動作を説明する。図9において、まず、アプリケーションが本人認証を要求する(ステップS81)。次に、アプリケーションが要求する本人確認レベルをカード側本人確認機能へ送信し(ステップS82)、カード内の認証方法が要求された本人確認レベルを満足するか否かを判定する(ステップS83)。ステップS83において、カード内の認証方法が要求された本人確認レベルを満足する場合(ステップS83のYES)、優先順位の高い認証方法を選択し(ステップS84)、選択された認証方法が実行可能であるか否かを判定する(ステップS85)。ステップS85において、選択された認証方法が実行可能である場合(ステップS85のYES)、指定された認証方法を実行する(ステップS86)。そして、認証が成功したか否かを判定する(ステップS

7)。ステップS87において、指定された認証が成功していた場合(ステップS87のYES)、アプリケーションに結果を返信する(ステップS88)。一方、ステップS83において、カード内の認証方法が要求された本人確認レベルを満足しない場合(ステップS83のNO)、あるいは、ステップS85において、選択された認証方法が実行不可能である場合(ステップS85のNO)、アプリケーションにエラーを返信し(ステップS89)、アプリケーション利用サービスを終了する。また、ステップS87において、指定された認証が成功していなかった場合(ステップS87のNO)、失敗を記録して(ステップS90)、アプリケーションに結果を返信する(ステップS88)。

【0029】次に、図10のフローチャートを用いて、本実施の形態のICカードで実行されるアプリケーションが複数の認証方法を優先順位により選択して実行する場合の動作を説明する。図10において、アプリケーションが本人認証を要求すると、優先順位1の認証方法を実行する(ステップS101)。次に、実行した認証方法の認証結果の本人確認レベルを求め、カード側本人確認レベルへ記録する(ステップS102)。次に、カード側本人確認レベルが、アプリケーションで要求された本人確認レベルを満たすか否かを判定する(ステップS103)。ステップS103において、求められた本人確認レベルがアプリケーションで要求された本人確認レベルを満たさないと判定した場合(ステップS103のNO)、優先順位に従い、本人確認レベルを満たす最適な認証方法を探索する(ステップS104)。次に、探索回数が予め設定された上限値を超えたか否かを判定し

(ステップS105)、探索回数が上限値を超えていない場合(ステップS105のNO)、探索した認証方法を実行して認証結果の本人確認レベルを算出し、カード側本人確認レベルへ加算する(ステップS106)。そして、加算されたカード側本人確認レベルが、アプリケーションで要求された本人確認レベルを満たすか否かを判定する(ステップS107)。

【0030】ステップS107において、求められた本人確認レベルがアプリケーションで要求された本人確認レベルを満たさないと判定した場合(ステップS107のNO)、ステップS104へ戻り、上述の動作を繰り返して本人確認レベルを加算して積み重ねる。一方、ステップS105において、探索回数が予め設定された上限値を超えていた場合(ステップS105のYES)、アプリケーションに認証エラーを通知して(ステップS108)終了する。また、ステップS103において、求められた本人確認レベルがアプリケーションで要求された本人確認レベルを満たすと判定した場合(ステップS103のYES)、あるいは、ステップS107において、求められた本人確認レベルがアプリケーションで要求された本人確認レベルを満たすと判定した場合(ステップS107のYES)、ICカード内に現在の本人確認レベルを設定して(ステップS109)アプリケーションの実行を行う。なお、上述の説明では、ステップS104において、優先順位に従って本人確認レベルを満たす最適な認証方法を探索する場合、探索回数を予め設定し、探索回数が設定された上限値を超えたか否かを、探索を続けるか否かの判定基準としたが、探索回数と同様に探索時間を設定し、探索時間が設定された上限時間を超えたか否かを、探索を続けるか否かの判定基準としても良い。

【0031】次に、図11のフローチャートを用いて、本実施の形態のICカードで実行される複数のアプリケーションが認証結果を共有する場合の動作を説明する。ここでは、複数のアプリケーションプログラムの中でユーザが最初に実行させるアプリケーションプログラムを“アプリケーション1”として説明を行う。図11において、まず、ユーザにアプリケーション1を選択させる(ステップS121)。次に、アプリケーション1が要求するカード側本人認証機能により本人認証を行い(ステップS122)、認証結果をカード側本人確認レベルへ記録する(ステップS123)。認証結果を記録したら、アプリケーション1を実行する(ステップS124)。次に、ユーザに続けて他のアプリケーションを実行するか否かを入力させる(ステップS125)。ステップS125において、ユーザが続けて他のアプリケーションを実行するとした場合(ステップS125のYES)、他のアプリケーションを選択させる(ステップS126)。他のアプリケーションが選択されたら、他のアプリケーションが要求する認証方法を確認する

(ステップS127)。次に、現在のカード側本人確認レベルを取得する(ステップS128)。現在のカード側本人確認レベルを取得したら、カード側本人確認レベルと他のアプリケーションに要求された本人確認レベルを比較し(ステップS129)、要求された本人確認レベルの方が大きいかな否かを判定する(ステップS130)。

【0032】ステップS130において、要求された本人確認レベルの方が大きい場合(ステップS130のYES)、要求された認証方法による本人認証を行い、カード側本人確認レベルを更新する(ステップS131)。ここで、カード側本人確認レベルの更新は、“本人確認レベル(更新後)=本人確認レベル(更新前)+他のアプリケーションの認証結果による本人確認レベル”とする。また、ここでは単純に加算をした例を示しているが、利用環境によって予め設定されている重み付け因子を掛け合わせた値を加算しても良い。本人確認レベルが更新されたら、他のアプリケーションを実行し(ステップS132)、ステップS125に戻って、ユーザに更なる他のアプリケーションを実行するか否かを入力させる。一方、ステップS125において、ユーザが続けて他のアプリケーションを実行しないとした場合(ステップS125のNO)、カード側本人確認レベルをクリアし(ステップS133)、アプリケーション利用サービスを終了する(ステップS134)。また、ステップS130において、要求された本人確認レベルの方が小さい場合(ステップS130のNO)、要求された認証方法による本人認証は行わず、他のアプリケーションを実行する(ステップS132)。

【0033】また、カード内の本人認証機能を使う場合、認証の失敗によりテンプレートがロックする場合がある。そこで、テンプレートがロックした場合においても、ユーザがカードを継続して利用できるよう、図12、及び図13のフローチャートを用いて、専用のメンテナンス装置によるICカードのカード所持者が行う本人認証機能のメンテナンス動作を説明する。図12において、まず、メンテナンス装置へICカードを挿入させる(ステップS141)。次に、ICカードメンテナンス認証を行う(ステップS142)。メンテナンス認証の方法は、図5で説明した認証方法をメンテナンス鍵により行うことが違うのみであるので、ここでは説明を省略する。メンテナンス認証を行ったら、認証が成功したか否かを判定する(ステップS143)。ステップS143において、メンテナンス認証が成功していた場合(ステップS143のYES)、ICカードに、ロックしていないテンプレートで本人認証を行わせる(ステップS144)。次に、本人認証が成功したか否かを判定する(ステップS145)。ステップS145において、本人認証が成功していた場合(ステップS145のYES)、現在ロックしているテンプレートの一覧を表

示する(ステップS146)。

【0034】ロックしているテンプレートの一覧を取得したら、アンロック可能なテンプレートがあるか否かを判定する(ステップS147)。ステップS147において、アンロック可能なテンプレートがある場合(ステップS147のYES)、図13に示すようにロックを解除する(ステップS148)。次に、ロックの解除が成功したか否かを判定する(ステップS149)。ステップS149において、ロックの解除が成功していた場合(ステップS149のYES)、テンプレートの再登録を実行する(ステップS150)。テンプレートの再登録を実行したら、テンプレートの再登録が成功したか否かを判定し(ステップS151)、成功していた場合(ステップS151のYES)、現在の登録状況を表示する(ステップS152)。そして、ICカードのテンプレートの登録状況を表示したら、ICカードを排出する(ステップS153)。

【0035】一方、ステップS143において、メンテナンス認証が成功していなかった場合(ステップS143のNO)、ICカードを取り込み、システムを停止して終了する(ステップS154)。また、ステップS145において、本人認証が成功していなかった場合(ステップS145のNO)、再度確認するか否かを確かめ(ステップS155)、再度確認する場合(ステップS155のYES)、ステップS144へ戻り、本人認証を再実行させる。ステップS155において、本人認証を再度確認しない場合(ステップS155のNO)、あるいは、ステップS147において、アンロック可能なテンプレートがない場合(ステップS147のNO)、ステップS153へ進み、ICカードを排出する。また、ステップS151において、テンプレートの再登録が成功していなかった場合(ステップS151のNO)、再度、再登録するか否かを確認する(ステップS156)。ステップS156において、再登録を行う場合(ステップS156のYES)、ステップS150へ戻り、上述の動作を繰り返す。ステップS156において、再登録を行わない場合(ステップS156のNO)、現在の登録状況を表示し(ステップS152)、ICカードを排出する(ステップS153)。

【0036】次に、図14のフローチャートを用いて、専用のメンテナンス装置によるICカードのシステム管理者が行う本人認証機能のメンテナンス動作を説明する。図14において、まず、メンテナンス装置へ管理者ICカードを挿入させる(ステップS161)。次に、ICカードに、ロックしていないテンプレートで本人認証を行わせ(ステップS162)、本人認証が成功したか否かを判定する(ステップS163)。ステップS163において、本人認証が成功していた場合(ステップS163のYES)、メンテナンス用の鍵を読み出す(ステップS164)。メンテナンス用鍵を取得した

ら、管理者ICカードを排出し(ステップS165)、ユーザ用のICカードを挿入させる(ステップS166)。そして、図12に示したステップS142に進み、ステップS142からステップS156までの上述の動作を行う。一方、ステップS163において、本人認証が成功していなかった場合(ステップS163のNO)、再度確認するか否かを確かめ(ステップS167)、再度確認する場合(ステップS167のYES)、ステップS162へ戻り、本人認証を再実行させる。ステップS167において、本人認証を再度確認しない場合(ステップS167のNO)、ICカードを排出する(ステップS168)。

【0037】(実施例の説明)次に、本発明の実施例を図面を参照して説明する。図15は、本発明の実施例のシステム構成を説明するブロック図である。本実施例は、ICカードを郵送や街角の自動販売機から入手する例を示す。図15において、符号101は、ICカードの発行とICカードのユーザ管理を行う顧客管理サーバを示す。符号102は、認証データを登録してICカードを発行する顧客管理サーバ101に接続された認証データ登録ICカード発行機を示す。符号103は、ICカードのユーザが顧客管理サーバへアクセスするためのクライアント端末を示す。符号104は、指紋情報等の認証用の情報を取得するためにクライアント端末103に接続されたスキャナまたは照合装置を示す。符号105は、現金の支払い機能の他に、カメラや指紋照合装置、暗証番号入力用の操作部等を備えたICカード自動販売機を示す。ICカード自動販売機では、個人がカードを購入する時には、必ずなんらかの認証方法を選択しなければICカードは購入できないものとする。符号106は、ICカード自動販売機で販売されたICカードの情報を管理するICカード販売管理サーバを示す。符号107は、顧客管理サーバ101と、クライアント端末103と、ICカード自動販売機105と、ICカード販売管理サーバ106との間を接続するコンピュータネットワークを示す。なお、クライアント端末103は、スキャナ、または照合装置が接続できればPC等の他、携帯端末でも良い。

【0038】次に、図16に示すシーケンス図を用いて、図15に示すシステムにおける認証データ登録ICカード発行機102によるICカード発行動作を説明する。図16において、まず、個人の自宅のパソコン(クライアント端末103)からダイヤルアップでプロバイダなどに接続し、インターネット上の顧客管理サーバ101が立ち上げているホームページに接続する。そして、認証機能登録のセッションを要求する(ステップS181)。セッションを要求された顧客管理サーバ101は、認証情報の入力をクライアント端末103を操作するユーザへ求める(ステップS182)。認証情報の入力を要求されたユーザは、クライアント端末103か

らID番号やパスワード等を送信する(ステップS183)。顧客管理サーバ101では、送信された認証情報によりユーザの認証を行い(ステップS184)、結果をクライアント端末103へ通知する(ステップS185)。認証結果を受けて、ユーザは次にクライアント端末103から、自分の氏名、電話番号の他、メールアドレス、ICカードの登録に必要な暗証番号などのパスワード等のICカードへの記録情報、本人が確認できる画像データ(運転免許証や保険証のコピー)や電子証明書等を送信する(ステップS186)。このときに、登録するICカードの種類や、価格、絵柄、メモリ容量を選択できるようにしても良い。また、ICチップとカードが分離できる場合は、バラバラに購入し、使用時に組み合わせても良い。

【0039】ICカードへの記録情報を受信した顧客管理サーバ101は、発信者番号通知により取得した電話番号や氏名と、入力された電話番号や氏名が一致することを確認してユーザを確認する(ステップS187)。ユーザが確認できたら、顧客管理サーバ101は、認証データ登録ICカード発行機102へ、顧客管理サーバ101で受信した本人が確認できる情報や画像、更にパスワード等のICカードへの記録情報を送信する(ステップS188)。次に、クライアント端末へ認証情報の登録の確認として、登録応答を送信する(ステップS189)。一方、認証データ登録ICカード発行機102は、顧客管理サーバ101から送信された認証情報等のデータを記録したICカードを発行し、顧客管理サーバ101に履歴を登録する(ステップS190)。その後、発行されたICカードは郵送等によりクライアント端末103を操作するユーザの元へ届けられ(ステップS191)、ユーザは必要に応じて本人認証データの再登録を行う(ステップS192)。送付されたICカードは、指定した暗証番号や、画像データが登録されているので、それらを用いて本人認証した後に、個人が選択する認証方法で、再登録することができる。例えば、自宅のパソコンに接続した本人認証装置から取り込んだ指紋データをICカードに再登録することで、指紋によるカード所持者確認も可能となる。なお、再登録の手続きは、個人が選択できる認証方法を一度しか変更できない設定にさせても良い。また、クライアントサーバ間でやり取りを行うデータは暗号化されていても良い。

【0040】次に、図17に示すシーケンス図を用いて、図15に示すシステムにおけるICカード自動販売機によるICカード入手動作を説明する。図17において、まず、ユーザが街角にあるICカード自動販売機105に行き、ICカードの購入を要求する(ステップS201)。ユーザにICカードの購入を要求されたICカード自動販売機105は、ICカード販売管理サーバ106へカード登録のセッションを要求する(ステップS202)。カード登録のセッションを要求されたICカー

ド販売管理サーバ106は、ICカード自動販売機105へセッションの要求応答を送信する(ステップS203)。ICカード販売管理サーバ106のセッション要求応答を受信したICカード自動販売機105は、ユーザへICカード購入要求の応答を表示する(ステップS204)。次に、ユーザはICカードに設定する認証方法を選択し(ステップS205)、必要な認証データ等のICカードへの記録情報を入力する(ステップS206)。ICカードへの記録情報を受信したICカード自動販売機105は、ICカードの発行・登録を行い(ステップS207)、発行したICカード情報をICカード販売管理サーバ106へ送信する(ステップS208)。ICカードの発行・登録情報を受信したICカード販売管理サーバ106は、ICカード自動販売機105へカード登録のセッション終了を送信する(ステップS209)。そして、ICカード自動販売機105は、作成されたICカードを排出して(ステップS210)ICカード販売の動作を終了する。

【0041】次に、このようにして入手したICカードの使用例を図面を用いて説明する。本使用例は、病気を患っているユーザが、遠い病院に薬をとりに行く手間は非常に大変であるので、病院が患者の住んでいる場所の近くのコンビニエンスストアに、当該患者の薬を運ぶサービスを行う例である。ICカード内には、ICカードにキャッシュカードアプリケーションが既に入っており、上記サービスを受けたい利用者は、病院等で病院のIDカードアプリケーションを入手し、近くのコンビニエンスストアへ薬を取りに行く。まず、図18から図21にICカード内のデータ構成の例を示す。図18は、本発明の実施例のICカード内アプリケーション構成例を説明する模式図である。図18において、ICカード内には、

(1)アプリケーションプログラムとして、“キャッシュカードアプリケーション”と後からダウンロードされた“病院用IDカードアプリケーション”が記録されている。それぞれのアプリケーションには、“a. 本人認証機能使用フラグ”と、“b. 本人確認レベル”が設定されており、病院用IDカードアプリケーションには、更に“c. 薬情報”が記録されている。

【0042】また、(2)認証方法に関する情報として、認証方法1を順位1、認証方法3を順位2、認証方法2を順位3とする“認証方法優先順位”と、認証方法1をパスワード、認証方法2を指紋照合、認証方法3を音声照合とする“カード側認証方法リスト”と、認証方法1のテンプレート及びパラメータと、認証方法2のテンプレート及びパラメータと、認証方法3のテンプレート及びパラメータが記録されている。図19は、図18におけるICカード内のパスワードによる認証方法リストの詳細を説明する模式図である。図20は、図18におけるICカード内の指紋照合による認証方法リストの詳細を説明する模式図である。図21は、図18にお

るICカード内の音声照合による認証方法リストの詳細を説明する模式図である。各図において、それぞれの認証方法は、“a. 認証方法用テンプレート”と、更に“b. 認証方法パラメータ”として、“しきい値”、“テンプレート優先順位”、“ロック再試行回数”、“アンロック再試行回数”、“アンロック回数上限値”、“ロック回数上限値”、“組み合わせパラメータ”の各パラメータが設定されている。上述の例では、ユーザが手を怪我しており指紋認証ができない状況が生じたため、指紋認証の順位を一番後ろになるように設定されている。

【0043】以上を前提に、本実施例の実施方法を示す。図22、及び図23は、ICカードに記録された病院用IDカードアプリケーションの動作を説明するシーケンス図である。図22において、まず、ユーザは自宅に用意されたクライアント端末103により、病院のホームページへアクセスし、ICカードを挿入して病院用アプリケーション（病院のホームページ）に薬購入のセッションを要求する（ステップS221）。病院用アプリケーションは、セッション要求に応答してICカード（病院用IDカードアプリケーション）に相互認証を要求する（ステップS222）。次に、ICカードと病院用アプリケーションは相互認証を行う（ステップS223）。なお、相互認証の詳細は後述する。相互認証が終了したら、病院用IDカードアプリケーションによる本人認証を行う（ステップS224）。ここでは、病院用IDカードアプリケーションが要求する本人確認レベルが、指紋認証、または音声認証とパスワードの併用のどちらか一方が必要であるため、上述のようにICカード内の優先順位の高い、パスワードと音声認証の併用を本人認証方法として選択する。当該認証方法にて本人確認を行い、認証が成功した段階で、病院内のホームページにログインができ、必要な薬の購入を病院のホームページから注文する（ステップS225）。

【0044】次に、病院用アプリケーションは、薬の在庫チェックを行い（ステップS226）、在庫が確認できれば購入代金の支払いを要求する（ステップS227）。購入代金の支払いを要求されたユーザは、キャッシュカードアプリケーションによる支払処理を行う（ステップS228）。なお、キャッシュカードアプリケーションによる支払処理の詳細は後述する。キャッシュカードアプリケーションによる支払処理後、ユーザは支払要求に対する応答を行い（ステップS229）、病院用アプリケーションは、ICカードに薬の予約情報を書き込む（ステップS230）。ICカードから予約情報書き込みに対する応答が送信されると（ステップS231）、病院用IDカードアプリケーションは、指定の店舗への薬の配送を行う（ステップS232）。

【0045】後日、ユーザは指定の店舗へ行き、店舗に用意されたクライアント端末103に対して薬購入のセ

ッションを要求する（ステップS233）。店舗端末（店舗用のアプリケーション）は、セッション要求に応答してICカードに相互認証を要求する（ステップS234）。次にICカードと店舗端末は相互認証を行う（ステップS235）。なお、相互認証の詳細は後述する。相互認証が終了したら、図23に示すように、薬の受け取りに必要な本人認証を行う（ステップS236）。ここでは、薬の受け取りに必要な本人確認レベルは、低く設定されているため、カードを持っていることによって本人認証がなされる。次に、店舗端末は薬の予約情報をICカードへ送信し（ステップS237）、ICカードは、カード側に登録されている薬情報と、届けられている薬との整合性を確認する（ステップS238）。そして、確認結果を店舗端末へ通知する（ステップS239）と同時に、店舗はカード所有者に当該の薬を手渡す（ステップS240）。なお、カード側に登録されている薬情報と、届けられている薬との整合性を確認できたら、ICカードは予約情報は削除する。

【0046】次に、図24、及び図25のシーケンス図を用いて、ICカードと病院または店舗用のアプリケーションとの相互認証動作の一例を説明する。図24において、まず、病院または店舗用のアプリケーションが、アプリケーション鍵を発行者鍵により暗号化し（ステップS241）、ICカードへ送信する（ステップS242）。ICカードは受信した暗号文を復号化し、アプリケーション鍵をICカードにセットする（ステップS243）。次に、病院または店舗用のアプリケーションは乱数Cを発生し（ステップS244）、ICカードへ生成した乱数Cを送信する（ステップS245）。乱数Cを受信したICカードは、アプリケーション鍵で乱数Cを暗号化し（ステップS246）、病院または店舗用のアプリケーションへ送信する（ステップS247）。病院または店舗用のアプリケーションは、受信した暗号文を復号化し（ステップS248）、復号化した乱数を生成した乱数Cと比較する（ステップS249）。ステップS249において、比較した乱数が一致した場合、病院または店舗用のアプリケーションは、アプリケーション鍵はICカードにセットされたと判断する（ステップS250）。ステップS249において、比較した乱数が一致しない場合、病院または店舗用のアプリケーションは、アプリケーション鍵はICカードにセットされないと判断する（ステップS251）。アプリケーション鍵がICカードにセットされない場合、ICカードは偽造である可能性がある。

【0047】次に、図25に示すように、ICカードが、カード鍵を発行者鍵により暗号化し（ステップS252）、病院または店舗用のアプリケーションへ送信する（ステップS253）。病院または店舗用のアプリケーションは受信した暗号文を復号化し、カード鍵を病院または店舗用のアプリケーションにセットする（ステッ

ブS254)。次に、ICカードは乱数Dを発生し(ステップS255)、病院または店舗用のアプリケーションへ生成した乱数Dを送信する(ステップS256)。乱数Dを受信した病院または店舗用のアプリケーションは、カード鍵で乱数Dを暗号化し(ステップS257)、ICカードへ送信する(ステップS258)。ICカードは、受信した暗号文を復号化し(ステップS259)、復号化した乱数を生成した乱数Dと比較する(ステップS260)。ステップS260において、比較した乱数が一致した場合、ICカードは、カード鍵は病院または店舗用のアプリケーションにセットされたと判断する(ステップS261)。ステップS260において、比較した乱数が一致しない場合、ICカードは、カード鍵は病院または店舗用のアプリケーションにセットされないと判断する(ステップS262)。カード鍵が病院または店舗用のアプリケーションにセットされない場合、病院または店舗用のアプリケーションは盗聴や改竄がされている可能性がある。

【0048】次に、図26のシーケンス図を用いて、本実施例のICカードのキャッシュカードアプリケーションの動作を説明する。図26において、まず、ユーザは自宅に用意されたクライアント端末103により、銀行用アプリケーションを起動し、ICカードを挿入してキャッシュカードアプリケーションによる銀行決済のセッションを要求する(ステップS281)。銀行用アプリケーションは、セッション要求に応答してICカードに本人認証を要求する(ステップS282)。ただし、ここでの本人確認は、既に病院用IDカードアプリケーションでの本人確認結果がカード内に存在しているため、図11のステップS130の手順に従えば、ここでの本人確認は省略が可能である。ICカードは正常に認証されたら、銀行用アプリケーションにステータスを送信する(ステップS283)。次に、銀行用アプリケーションはICカードの情報読み出しを行う(ステップS284)。ICカードは情報の読み出しに応答して、ユーザの口座情報や信用情報を銀行端末へ送信する(ステップS285)。この時、送信する情報は暗号化しても良い。次に、銀行用アプリケーションは、銀行端末へ振込先情報を送信する(ステップS286)。ユーザの情報と振込先情報を受信した銀行端末は、口座振替処理を行い(ステップS287)、振替結果をICカードへ通知する(ステップS288)。口座振替通知を受信したICカードは、口座振替結果を記録し(ステップS289)、銀行用アプリケーションへステータスを送信して(ステップS290)、ICカードのキャッシュカードアプリケーションを終了する。

【0049】次に、図27のフローチャートを用いて、本実施例のようにICカード内に2つのテンプレートが存在する場合のテンプレート選択動作を説明する。図27において、まず、第1テンプレートを用いて本人認証

を行う(ステップS301)。次に、認証が成功したか否かを判定する(ステップS302)。ステップS302において、認証が成功していなかった場合(ステップS302のNO)、第1のテンプレートによる認証回数を示すカウンタがN以上か否かを判定する(ステップS303)。ステップS303において、カウンタがN未満であった場合(ステップS303のNO)、ステップS301へ戻り、上述の第1テンプレートによる本人認証を繰り返す。ステップS303において、カウンタがN以上であった場合(ステップS303のYES)、次のテンプレートによる認証を行うか否かをユーザに入力させる(ステップS304)。ステップS304において、ユーザが次のテンプレートによる認証を行うとした場合(ステップS304のYES)、第2テンプレートを用いて本人認証を行う(ステップS305)。次に、認証が成功したか否かを判定する(ステップS306)。ステップS306において、認証が成功していなかった場合(ステップS306のNO)、第2のテンプレートによる認証回数を示すカウンタがN以上か否かを判定する(ステップS307)。ステップS307において、カウンタがN未満であった場合(ステップS307のNO)、ステップS305へ戻り、上述の第2テンプレートによる本人認証を繰り返す。ステップS307において、カウンタがN以上であった場合(ステップS307のYES)、本人認証の失敗を記録し(ステップS308)、アプリケーションに結果を返す(ステップS309)。一方、ステップS302において、認証が成功していた場合(ステップS302のYES)、ステップS308へ進み、アプリケーションに結果を返す。また、ステップS306において、認証が成功していた場合も(ステップS306のYES)、ステップS308へ進み、アプリケーションに結果を返す。

#### 【0050】

【発明の効果】以上の如く本発明によれば、サービス提供者毎に別々の本人認証方法を用いるのではなく、複数のサービスから、ICカード内の本人認証機能を共有することで、本人認証機能の無駄を省くことが可能となり、かつ、サービス利用者自身が複数の本人認証方法を、安全性を損なわない範囲で選択できる仕組みにより、本人認証に必要な情報の登録及び変更を容易に実現することが可能となる。従って、認証に対するなりすましの危険性を回避し、また、生体情報を利用する場合、怪我等の使用部位の状態、体調、更には指紋認証を例にとると、生まれつき指紋が薄くて認証には適さない等、生まれながらの特性により完全な本人認証ができない場合に対応するICカード、登録装置、及びサービス提供システムを実現できるという効果が得られる。

#### 【図面の簡単な説明】

【図1】 本発明の実施の形態のICカード上に構成される機能ブロックを説明するブロック図である。

10

20

30

40

50

【図 2】 同実施の形態の IC カード上の EEPROM に記録される情報の構成を説明する模式図である。

【図 3】 同実施の形態の IC カード上の EEPROM に記録される情報の構成を説明する模式図である。

【図 4】 同実施の形態の IC カードへの本人認証機能の登録動作を説明するフローチャートである。

【図 5】 本人認証機能の登録時の IC カードへの登録認証動作の一例を説明するシーケンス図である。

【図 6】 同実施の形態の IC カードへのアプリケーションプログラムの登録・削除動作を説明するフローチャートである。

【図 7】 アプリケーションの登録・削除時のアプリケーション鍵による認証動作の一例を説明するシーケンス図である。

【図 8】 アプリケーションの登録・削除時のアプリケーション鍵による認証動作の一例を説明するシーケンス図である。

【図 9】 同実施の形態の IC カードで実行されるアプリケーションが 1 つの認証方法を実行する場合の動作を説明するフローチャートである。

【図 10】 同実施の形態の IC カードで実行されるアプリケーションが複数の認証方法を優先順位により選択して実行する場合の動作を説明するフローチャートである。

【図 11】 同実施の形態の IC カードで実行される複数のアプリケーションが認証結果を共有する場合の動作を説明するフローチャートである。

【図 12】 同実施の形態の IC カードのカード所持者による本人認証機能のメンテナンス動作を説明するフローチャートである。

【図 13】 同実施の形態の IC カードのカード所持者による本人認証機能のメンテナンス動作を説明するフローチャートである。

【図 14】 同実施の形態の IC カードのシステム管理者による本人認証機能のメンテナンス動作を説明するフローチャートである。

【図 15】 本発明の実施例のシステム構成を説明するブロック図である。

【図 16】 本発明の実施例の認証データ登録 IC カード発行機による IC カード発行動作を説明するシーケンス図である。

【図 17】 本発明の実施例の IC カード自販機による

IC カード入手動作を説明するシーケンス図である。

【図 18】 本発明の実施例の IC カード内アプリケーション構成例を説明する模式図である。

【図 19】 本発明の実施例の IC カード内のパスワードによる認証方法リストの詳細を説明する模式図である。

【図 20】 本発明の実施例の IC カード内の指紋照合による認証方法リストの詳細を説明する模式図である。

【図 21】 本発明の実施例の IC カード内の音声照合による認証方法リストの詳細を説明する模式図である。

【図 22】 本発明の実施例の病院用 IC カードアプリケーションの動作を説明するシーケンス図である。

【図 23】 本発明の実施例の病院用 IC カードアプリケーションの動作を説明するシーケンス図である。

【図 24】 IC カードと病院または店舗用のアプリケーションとの相互認証動作の一例を説明するシーケンス図である。

【図 25】 IC カードと病院または店舗用のアプリケーションとの相互認証動作の一例を説明するシーケンス図である。

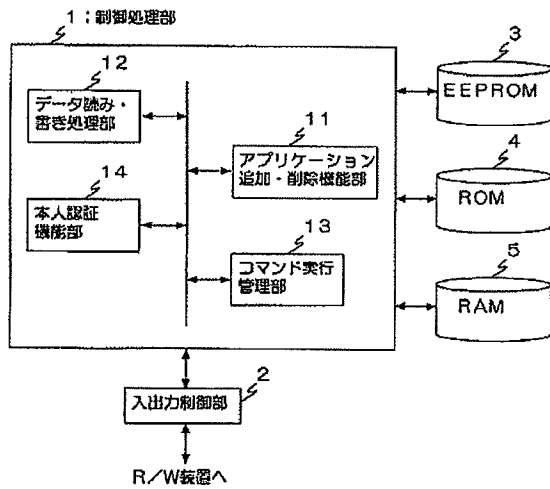
【図 26】 本発明の実施例のキャッシュカードアプリケーションの動作を説明するシーケンス図である。

【図 27】 本発明の実施例の IC カード内に 2 つのテンプレートが存在する場合のテンプレート選択動作を説明するフローチャートである。

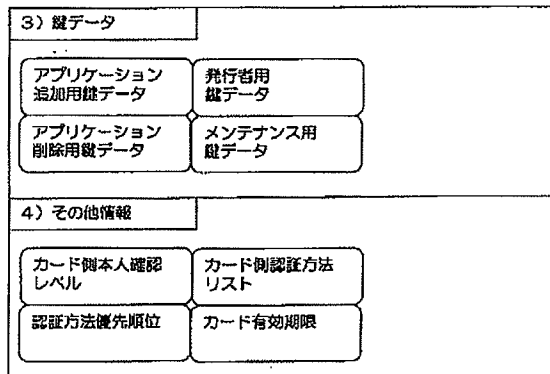
【符号の説明】

- |     |                   |
|-----|-------------------|
| 1   | 制御処理部             |
| 2   | 入出力制御部            |
| 3   | EEPROM            |
| 4   | ROM               |
| 5   | RAM               |
| 11  | アプリケーション追加・削除機能部  |
| 12  | データ読み・書き処理部       |
| 13  | コマンド実行管理部         |
| 14  | 本人認証機能部           |
| 101 | 顧客管理サーバ           |
| 102 | 認証データ登録 IC カード発行機 |
| 103 | クライアント端末          |
| 104 | スキャナまたは照合装置       |
| 105 | IC カード自動販売機       |
| 106 | IC カード販売管理サーバ     |
| 107 | コンピュータネットワーク      |

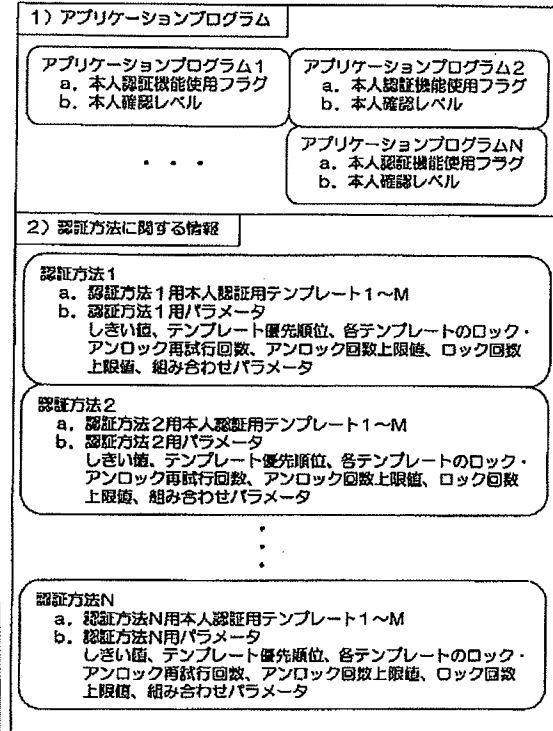
【図1】



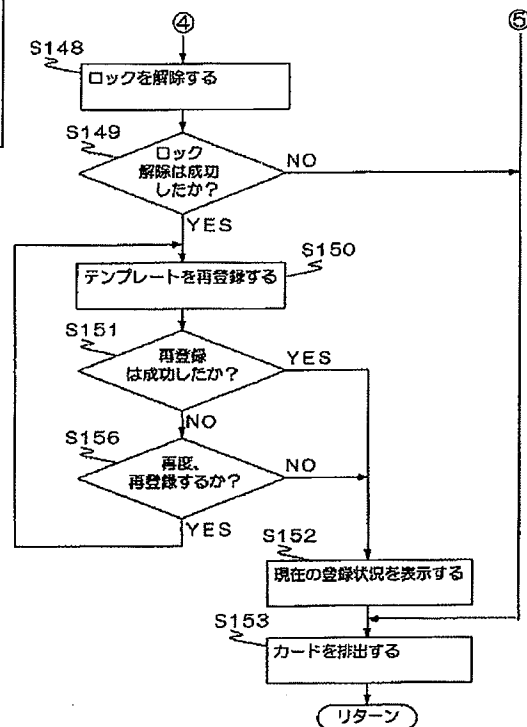
【図3】



【図2】

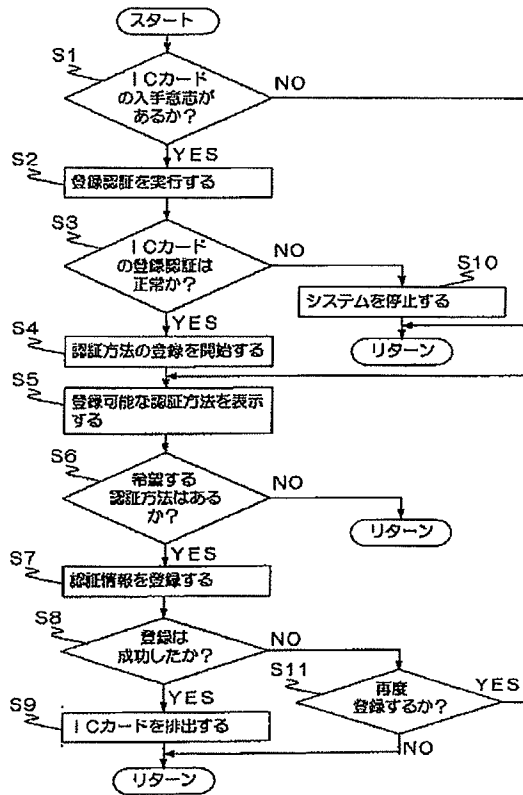


【図13】

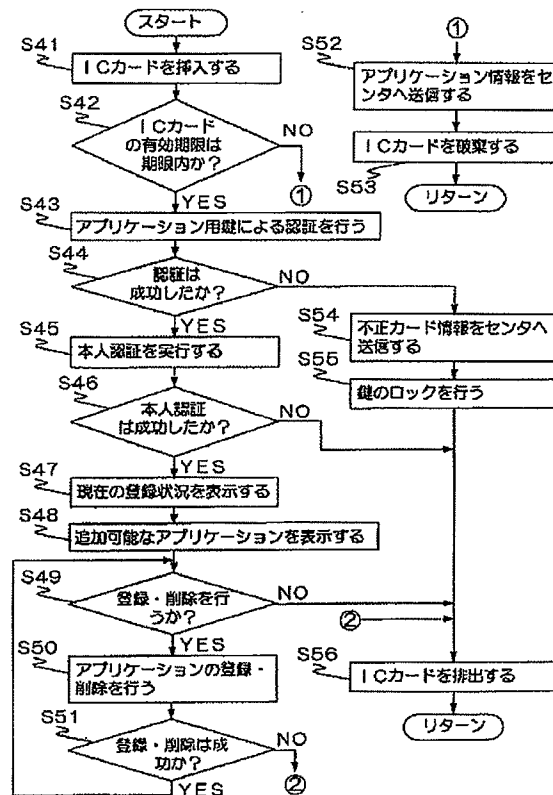




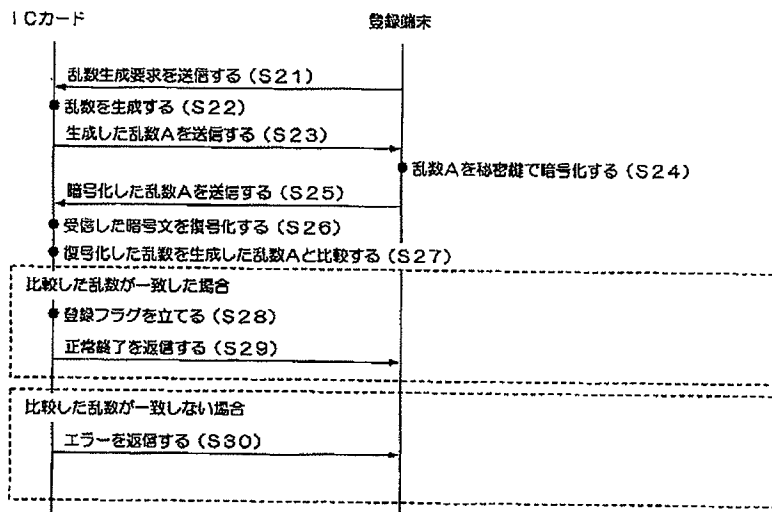
【図4】



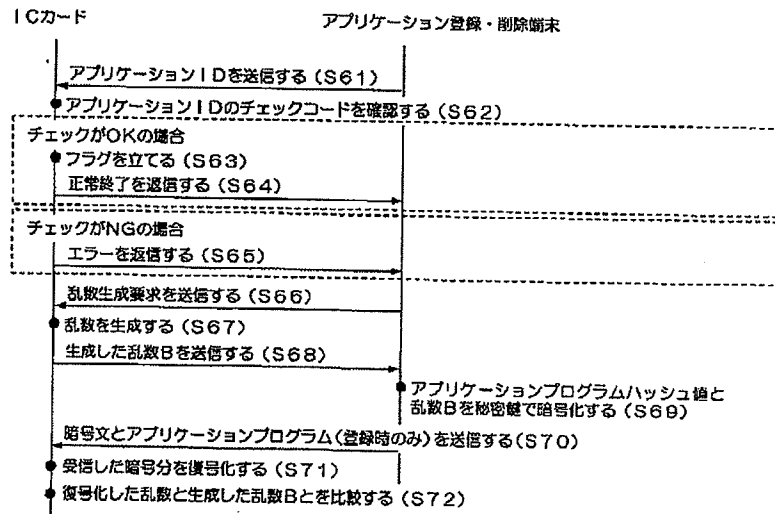
【図6】



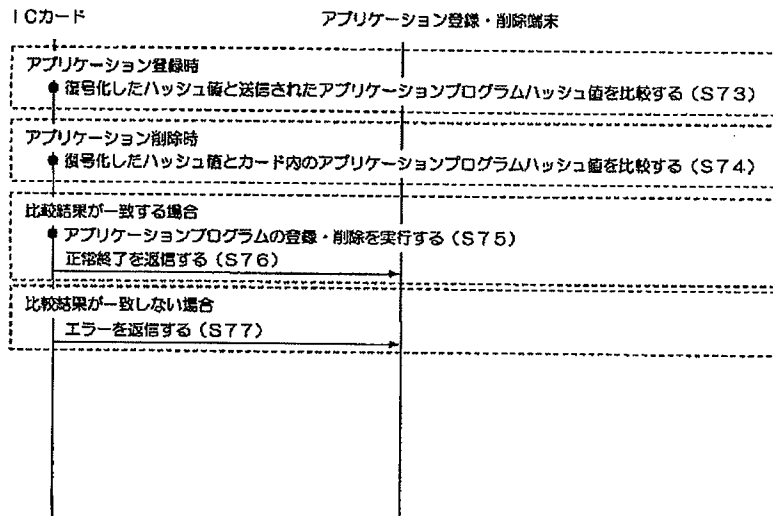
【図5】



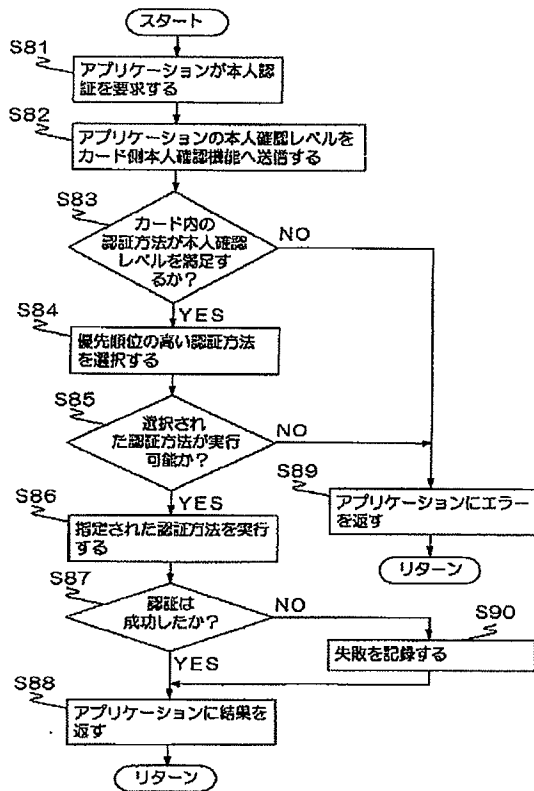
【図7】



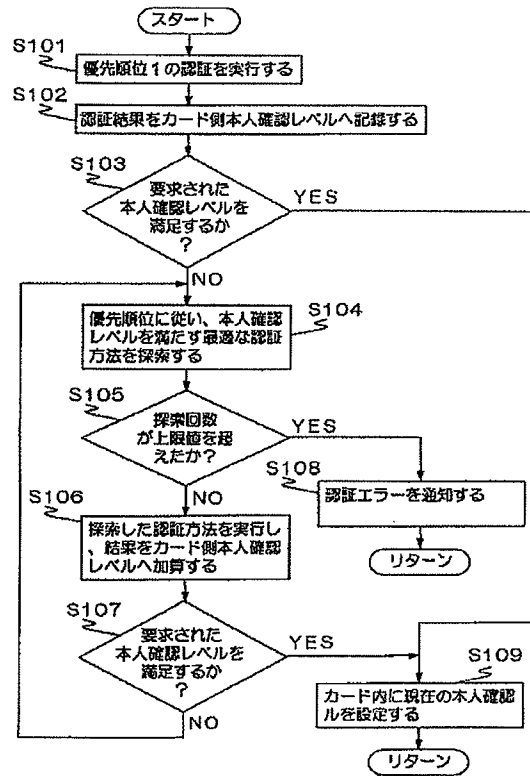
【図8】



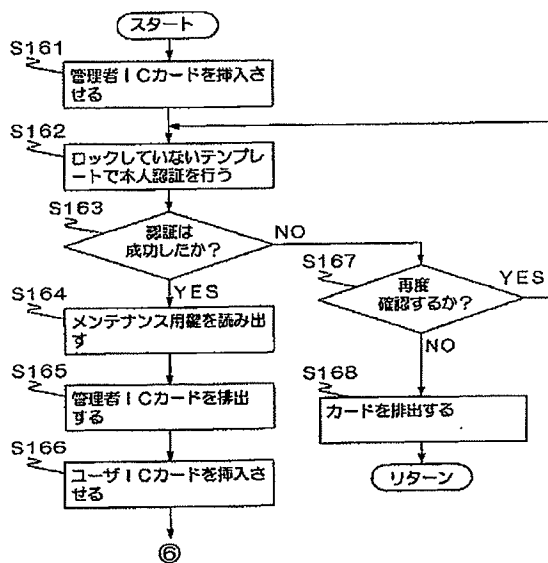
【図9】



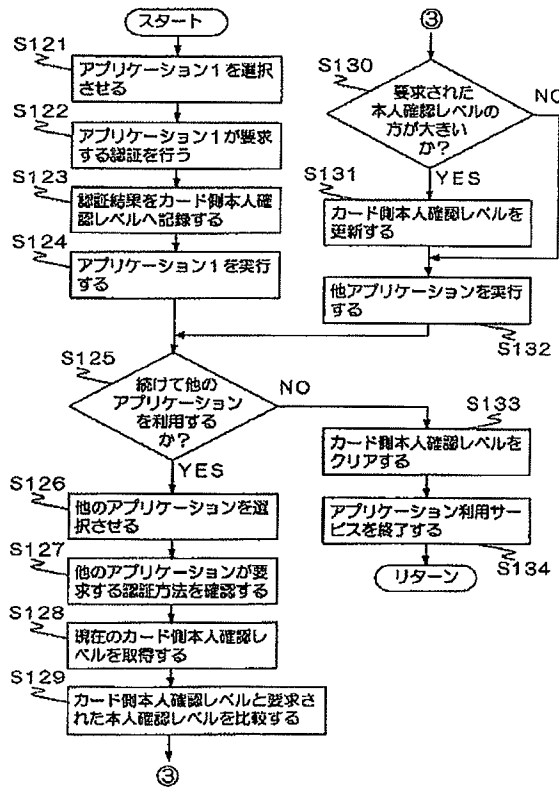
【図10】



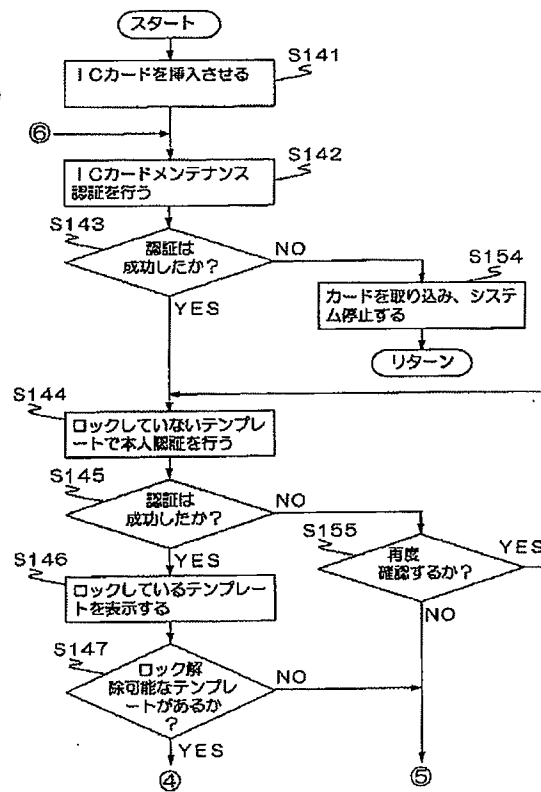
【図14】



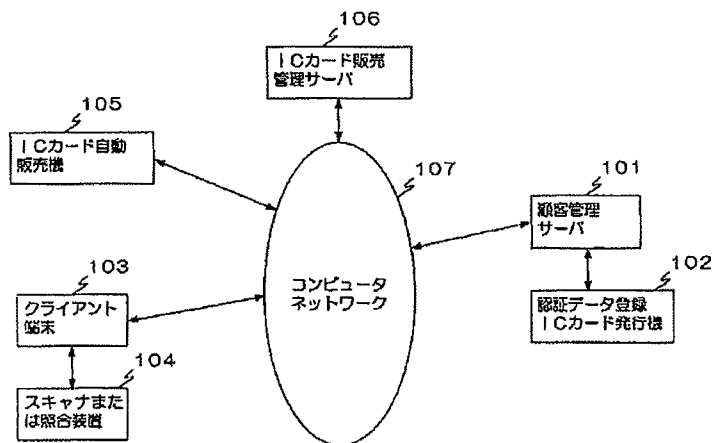
【図11】



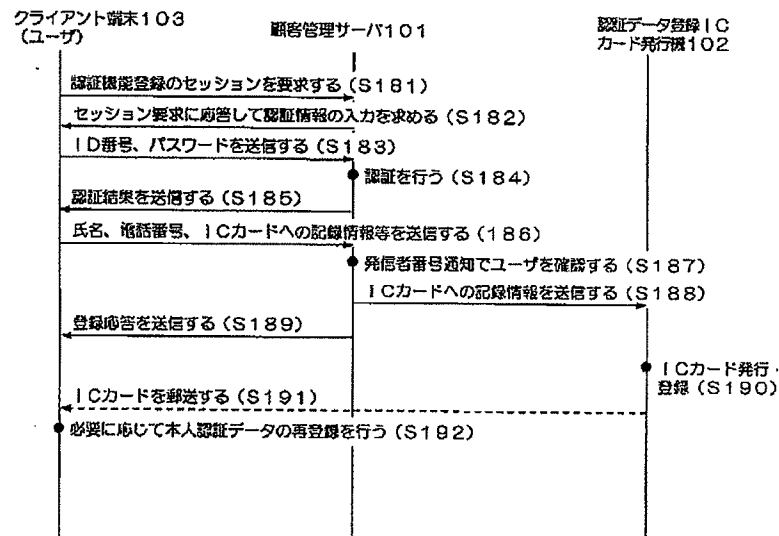
【図12】



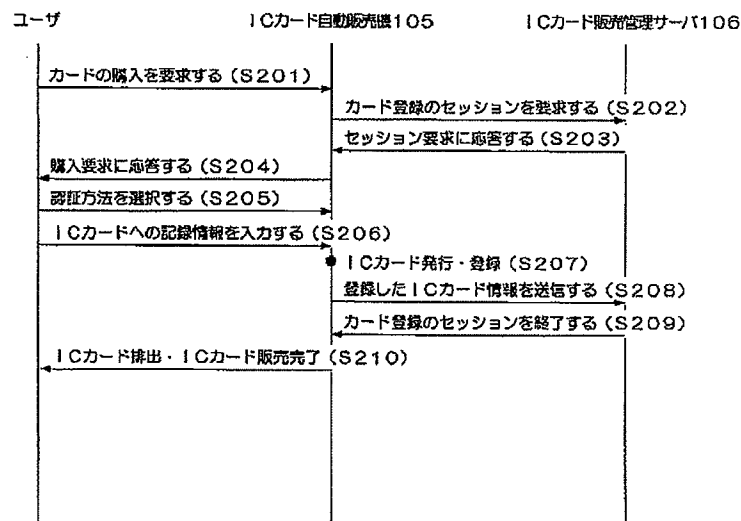
【図15】



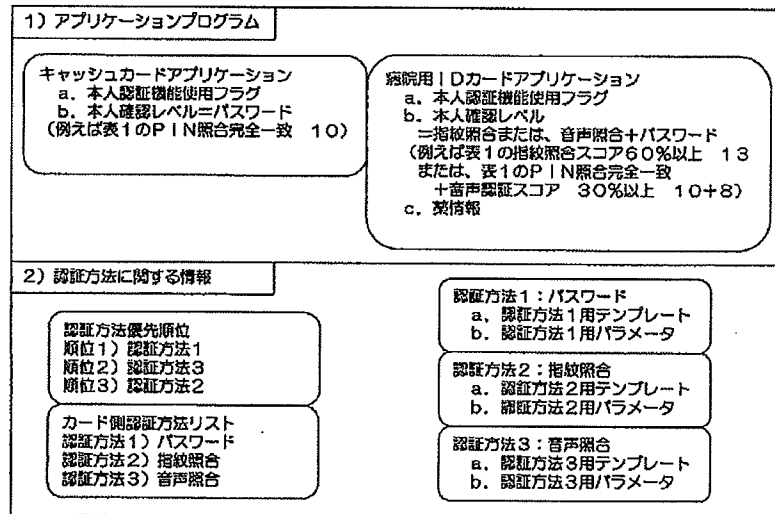
【図16】



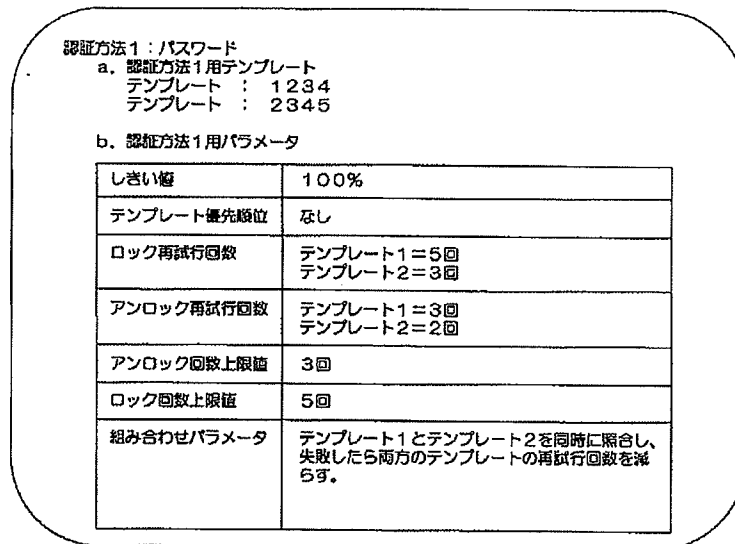
【図17】



【図18】



【図19】



【図20】

## 認証方法2：指紋照合

## a. 認証方法2用テンプレート

左手人差し指テンプレート : \*\*\*\*\*... \*\*  
 右手人差し指テンプレート : \*\*\*\*\*... \*\*

## b. 認証方法2用パラメータ

しきい値	75%
テンプレート優先順位	2
ロック再試行回数	テンプレート1=10回 テンプレート2=9回
アンロック再試行回数	テンプレート1=3回 テンプレート2=2回
アンロック回数上限値	3回
ロック回数上限値	10回
組み合わせパラメータ	優先順位の早い順に、一指づつ照合する。 一指に3回失敗したら、次の指の照合に入る。 次の指の照合を行うかは、外部からの信号による。

【図21】

## 認証方法3：音声照合

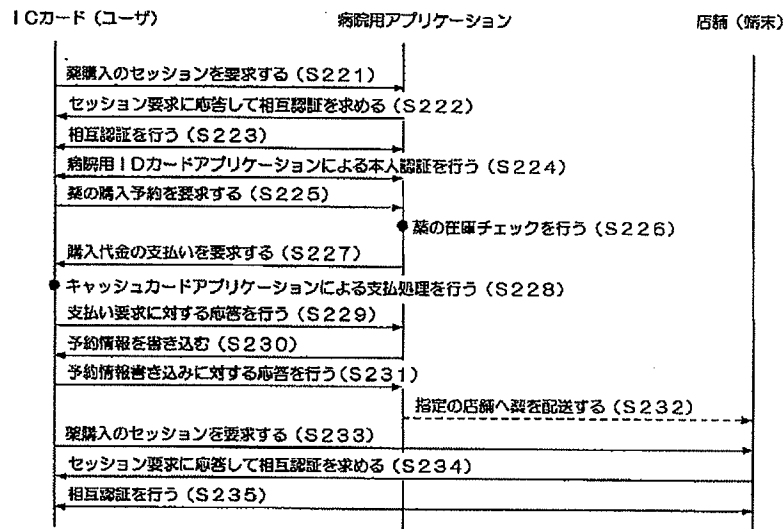
## a. 認証方法3用テンプレート

音声テンプレート : \*\*\*\*\*... \*\*  
 音声テンプレート : \*\*\*\*\*... \*\*

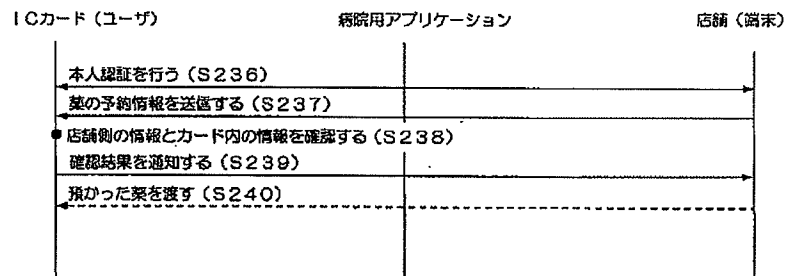
## b. 認証方法3用パラメータ

しきい値	40%
テンプレート優先順位	1
ロック再試行回数	テンプレート1=15回 テンプレート2=14回
アンロック再試行回数	テンプレート1=5回 テンプレート2=5回
アンロック回数上限値	5回
ロック回数上限値	15回
組み合わせパラメータ	両方の音声テンプレートを続けて照合し、 両方の類似度の平均がしきい値以上であることを 確認する。

【図22】

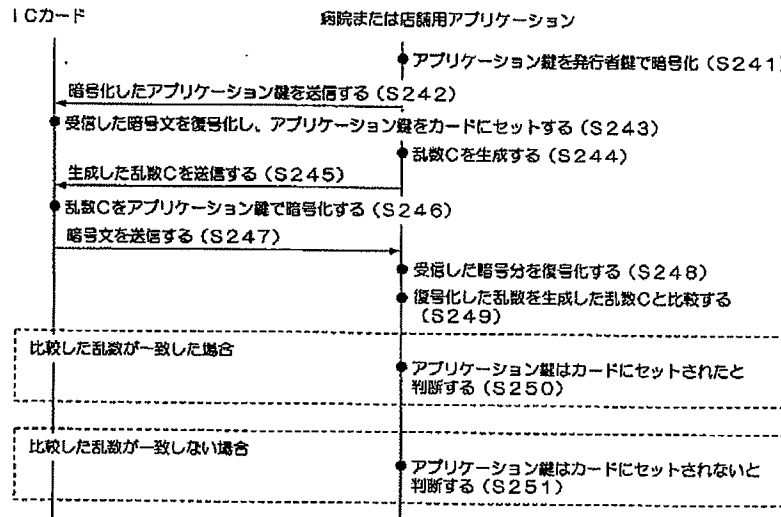


【図23】

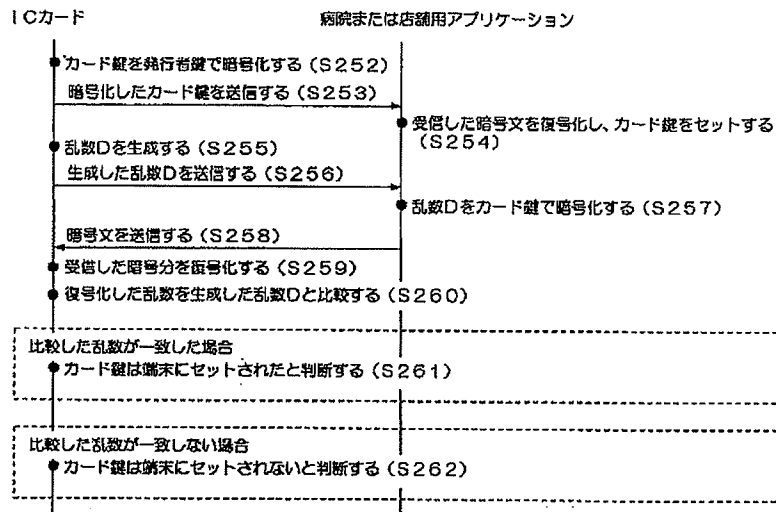




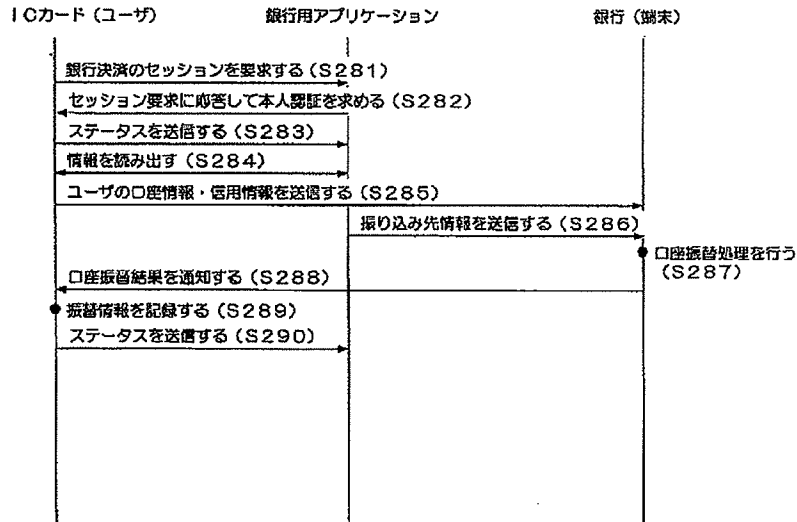
【図24】



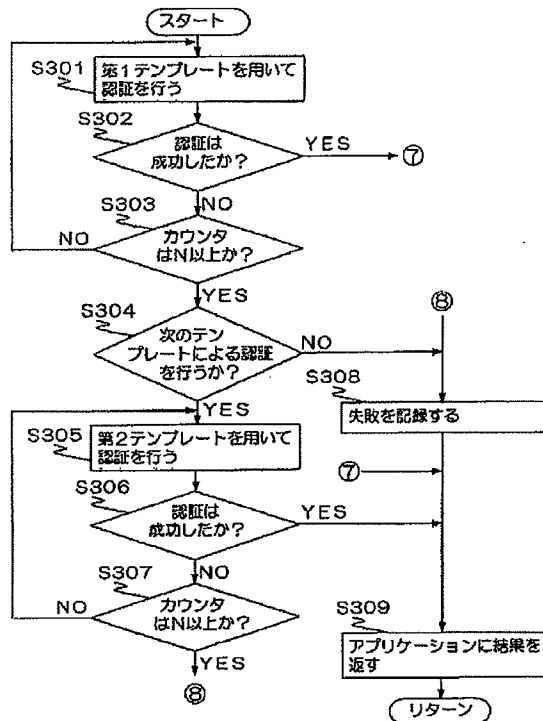
【図25】



【図26】



【図27】



フロントページの続き

F ターム(参考) 2C005 MA04 SA11  
5B035 AA14 BB09 BC01 CA38  
5B055 BB10 EE03 HA01 HA14 KK05  
KK13 KK14  
5B076 FB05  
5B085 AE12